

COMPUTING DEVICE WITH ENVIRONMENT AWARE FEATURES

BACKGROUND OF THE INVENTION

[0001] The present invention relates to computing devices that are used in changing environments.

[0002] The versatility of and uses for mobile electronic devices, and in particular such devices that are processor based and enabled for wireless communications, continue to expand. In many cases, utility features or mechanisms that are applied to mobile communications devices are often just substantial copies of those applied to conventional desktop computers. In such cases, the utility features do not take into consideration or take advantage of the aspects of mobile communications devices that are unique over stationary desktop devices. For example, password locking mechanisms on mobile communications devices such as handheld devices are substantially just a copy of the password locking mechanism used by a desktop, wherein the handheld device will lock up if it has not received an input from the user for a configurable amount of time. For example, if the mobile device keyboard has not been used for 30 minutes, it will lock up and the user will have to enter a password or special key combination to unlock it. Such a locking mechanism fails to exploit the differences between a mobile device and a stationary desktop computer.

[0003] Thus, there is a need for utility features for mobile communications devices that take advantage of the unique aspects of mobile devices to provide increased convenience for the user of the device and/or increased security. For example, a device locking mechanism designed for use in the mobile environment is desired, as are other mechanisms.

SUMMARY OF THE INVENTION

[0004] According to various example embodiments of the invention, utility features of a computing device, such as a password based locking mechanism or a mail filtering mechanism, are configured to automatically adjust based on the environment of the computing device.

[0005] According to one example aspect, an electronic device that includes a processor, an output device connected to the processor for issuing a stimulus to a user of the device, at least one input device connected to the processor and responsive to user input activity, and a device lock module associated with the processor for (i) implementing restrictions on user access to the device if user input activity falls below a threshold; and (ii) redetermining the threshold if a stimulus is issued by the output device.

[0006] According to another example embodiment, a method for providing security for a mobile communications device, including steps of: monitoring for predetermined user interaction with the mobile communications device; locking the mobile communications device if the predetermined user interaction is not detected within a predetermined lockout time interval; and resetting the lockout time interval to a shorter value if a user stimulus is issued by the mobile communications device.

[0007] According to another example aspect, a mobile device that includes a processor, at least a first input device connected to the processor for providing input signals thereto, an output device connected to the processor for providing output to a user of the mobile device, the processor being configured for determining location information for the mobile device based on input signals received from the first input device and adjusting an operating characteristic of the electronic device based on the determined location information.

[0008] According to another example embodiment, a method for providing security to a mobile electronic device including steps of: receiving input signals from an input device of the mobile electronic device; determining if the mobile electronic device is in a secure location based on the input signals; and applying a first security setting to the mobile electronic device if it is in the secure location and applying a second security setting to the mobile electronic device if it is not in the secure location.

[0009] Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Embodiments of the invention will now be described, by way of example only, with reference to the attached Figures, wherein:

[0011] Figure 1 is a block diagram showing a communications system including a mobile communications device to which the present invention may be applied;

[0012] Figure 2 is a flow diagram of a device lock process taken at the mobile communications device according to embodiments of the invention;

[0013] Figure 3 is a flow diagram of a further device lock process taken at the mobile communications device according to embodiments of the invention; and

[0014] Figure 4 is a flow diagram of another device lock process taken at the mobile communications device according to embodiments of the invention.

[0015] Like reference numerals are used throughout the Figures to denote similar elements and features.

DETAILED DESCRIPTION

[0016] Referring now to the drawings, Figure 1 is a block diagram of a mobile communication device 10 to which the invention is applied in an example embodiment. In an example embodiment, the mobile communication device 10 is a two-way communication device having at least data and, in some cases, also voice communication capabilities. In the example embodiment, the device 10 has the capability to communicate with other computer systems on the Internet.

Depending on the functionality provided by the device, in various embodiments the device may be a data communication device, a multiple-mode communication device configured for both data and voice communication, a mobile telephone, a PDA (personal digital assistant) enabled for wireless communication, a PDA not enabled for wireless communication, or a computer system with or without a wireless modem, among other things.

[0017] The device 10 includes a communication subsystem 11 for exchanging signals with a wireless communication network 50. As will be apparent to those

skilled in the field of communications, the particular design of the communication subsystem 11 will be dependent upon the communication network in which the device 10 is intended to operate.

[0018] The device 10 includes a microprocessor 38 that controls the overall operation of the device. The microprocessor 38 interacts with communications subsystem 11 and also interacts with further device subsystems such as the display 22, flash memory 24, random access memory (RAM) 26, auxiliary input/output (I/O) subsystems 28 (such as a thumbwheel or a vibration actuator, for example), serial port 30, keyboard or keypad 32, speaker 34, microphone 36, short-range communications subsystem 40, global Positioning System receiver (GPS Rx) 70 and any other device subsystems generally designated as 42.

[0019] Some of the subsystems shown in Fig. 1 perform communication-related functions, whereas other subsystems may provide "resident" or on-device functions. Notably, some subsystems, such as keyboard 32 and display 22 for example, may be used for both communication-related functions, such as entering a text message for transmission over a communication network, and device-resident functions such as a calculator or task list.

[0020] Operating system software 54 and various software applications 58 used by the microprocessor 38 are, in one example embodiment, stored in a persistent store such as flash memory 24 or similar storage element. Those skilled in the art will appreciate that the operating system 54, specific device applications 58, or parts thereof, may be temporarily loaded into a volatile store such as RAM 26. It is contemplated that received communication signals may also be stored to RAM 26.

[0021] The microprocessor 38, in addition to its operating system functions, preferably enables execution of software applications 58 on the device. A predetermined set of applications 58 which control basic device operations, including at least data and voice communication applications for example, will normally be installed on the device 10 during manufacture. Further applications may also be loaded onto the device 10 through the network 50, an auxiliary I/O subsystem 28, serial port 30, short-range communications subsystem 40 or any

other suitable subsystem 42, and installed by a user in the RAM 26 or a non-volatile store for execution by the microprocessor 38. Such flexibility in application installation increases the functionality of the device and may provide enhanced on-device functions, communication-related functions, or both. For example, secure communication applications may enable electronic commerce functions and other such financial transactions to be performed using the device 10.

[0022] In a data communication mode, a received signal such as a text message or web page download will be processed by the communication subsystem 11 and input to the microprocessor 38, which will preferably further process the received signal for output to the display 22, or alternatively to an auxiliary I/O device 28. A user of device 10 may also compose data items such as email messages for example, using the keyboard 32 in conjunction with the display 22 and possibly an auxiliary I/O device 28. Such composed items may then be transmitted over a communication network through the communication subsystem 11.

[0023] In some embodiments, for example in a personal digital assistant (PDA)-type communication device, the serial port 30 in Figure 1 may be used to permit synchronization with a user's desktop computer 72. Such a port 30 would enable a user to set preferences through an external device or software application and would extend the capabilities of the device by providing for information or software downloads to the device 10 or uploads from the device 10 other than through a wireless communication network.

[0024] A short-range communications subsystem 40 is a further component which may provide for communication between the device 10 and different systems or devices, which need not necessarily be similar devices. For example, the subsystem 40 may include an infrared device and associated circuits and components or a Bluetooth™ communication module to provide for communication with similarly enabled systems and devices. The device 10 may be a handheld device.

[0025] In some example embodiments, the device 10 includes a GPS receiver 70 for receiving location information from GPS satellites, thus enabling the device 10 to track its current location with a great deal of accuracy.

[0026] Wireless mobile network 50 is, in an example embodiment, a wireless packet data network, (e.g. Mobitex™ or DataTAC™), which provides radio coverage to mobile devices 10. Among other things, wireless mobile network 50 may also be a voice and data network such as GSM (Global System for Mobile Communication) and GPRS (General Packet Radio System), CDMA (Code Division Multiple Access), or various other third generation networks such as EDGE (Enhanced Data rates for GSM Evolution) or UMTS (Universal Mobile Telecommunications Systems).

[0027] In one example embodiment, the wireless network 50 is connected through one or more intermediate components 62 to one or more servers 68, which may be mail servers and/or access points for an intranet, the Internet, and/or other networks. Intermediate components 62 may include one or more gateways and/or connector systems as required to facilitate communications through the wireless network 50 with a plurality of mobile devices 10. The configuration of intermediate components 62 will depend on the desired functionality of the communications system and the type of wireless network 50, among other things.

[0028] In an example embodiment, among the software applications resident on the device 10 are one or more utility applications or modules 60. In various embodiments, utility applications may be stand alone applications, or may be sub-applications included as part of one or more larger software applications, or may be sub-applications integrated into operating system 54.

[0029] In an example embodiment, one of the utility applications is a device lock application or module 65 for locking the input and output interfaces of the mobile device 10 upon the occurrence of one or more predetermined conditions. Once the device has been locked, the user must enter use a password to unlock it. As known in the art, device lock mechanisms are used to prevent unauthorized access, and typically can either be manually triggered by the user (for example,

by using the "Lock Computer" function in Microsoft™ Windows™) or automatically triggered by a period of mouse/keyboard inactivity for a user configured time period. Unlike conventional device lock mechanisms, according to example embodiments, the device lock module 85 of the present invention automatically adapts its device lock behaviour based on the environment of the device 10.

[0030] Figure 2 shows an example device lock process, shown generally by reference 200, and performed by the device 10 when microprocessor 38 executes instructions to implement the device lock module 65. The device lock process 200 is a context aware process in that the timing of the locking action depends on user activity or lack thereof in response to a stimulus. The device lock process 200 attempts to distinguish between two different cases where a mobile communications device has not been subjected to any user actions for a duration of time. In one case, the device is not being used because the user is not close to it – in such a case it is desirable to lock the device as quickly as possible as it may be in an unsecured setting and thus require a high degree of security protection. In the alternative case, the device is in the immediate possession or proximity of the user, however the device is not being used because the user has had no need or desire to use it – for example, the user has not been prompted by any new emails, messages, phone calls or calendar reminders and has not sent any emails or made any phone calls or otherwise interacted with the device 10. In this alternative case, the device 10 is presumably in a safe setting with the user and an immediate device lock is not required.

[0031] By distinguishing between the above two cases, a device lock mechanism that balances convenience and security can be provided. For example, in a device lock mechanism that does not distinguish between the two cases, greater security can be provided by always locking a device after a relatively short period of user inactivity; however such locking can be inconvenient and unnecessary when the user of the device is right next to it. In order to distinguish between the two cases, according to aspects of the present

invention an assumption is made that a user of a device will generally respond and interact with the device when issued a stimulus. For example, events on the device such as an incoming phone call or a new email or a calendar reminder will typically be accompanied by a stimulus such as an audible sound such as a beep or a physical prompt such as a vibration, and if the user is close to or wearing the device he or she will generally interact with it shortly after receiving the stimulus. Thus, the process 200 assumes that if the user does not react to a stimulus than the device 10 is not near the user. Based on such assumption, the device lock process 200 is configured to use a shorter timeout setting for locking the device after a stimulus is issued than is used if a stimulus is not issued.

[0032] As indicated in Figure 2, the process 200 starts by setting a device lock timeout counter or timer to be equal to a predetermined default timeout value (step 202). The default timeout value is user configurable in an example embodiment - by way of non-limiting example it may be 30 minutes or such other value as the user deems appropriate or as is set automatically when the lock-out module 65 is configured or installed on the device 10. As indicated in step 204, the process 200 checks to see if the user has interacted with the device. The user interaction could for example include, among other things, pressing one or more keys on a keyboard or keypad, pressing or rotating an auxiliary input device 28 such as a thumbwheel, pressing a touch-screen, pressing a touchpad, moving a joystick, or otherwise activating any other form of user input mechanism of the device 10.

[0033] If a user input is detected in step 204, the process 200 determines that there is no need to lock the device, and returns to step 202 to reset the device lock timer back to the default timeout value. In the event that no user input is detected in step 204, the device lock timer is decremented (step 206), and then a check is done to determine if time has run out on the device lock timer (step 208). In the event that a timeout has occurred, the device 10 is locked (step 212). Locking of the device 10 will generally prevent anyone from viewing any files, messages or any other information that is stored on the locked device, as well as preventing any email or other messages from being composed or sent, and/or

phone calls from being made from the device (except, in some embodiments selected calls such as 911 emergency calls for example may still be permitted from a locked device). Locking of the device 10 effectively prevents the user from entering information into or extracting information out of the device, other than to enter a password or provide some other predetermined user input in order to unlock the device.

[0034] Turning again to step 208, in the event that the device lock timer has not run out of time, a check is done to determine if a user stimulus has recently been issued by the mobile device 10. A user stimulus includes attempts by the device 10 to get the attention of a user that may not be currently looking at the device, and in an example embodiment, the user stimulus includes, for example, an audible prompt such as a beep or ring, or a physical prompt such as a vibration. Such prompts may be issued by other applications running on the mobile device 10 for a variety of reasons – for example, stimuli may be issued in response to a new incoming email or other message received over wireless network 50, to announce an incoming phone call or a page, or to issue a reminder of an event scheduled in a calendar-type or to-do-list type of application. If no stimulus has been issued to the user, the process 200 loops back to step 204 and repeats steps 204-210 as set out above. If, however, a stimulus has been issued to the user, the timeout timer is set to a new time out value, namely a “stimulus reaction delay” setting value (step 214) prior to looping back to step 204. In an example embodiment, the timeout timer is only set to the stimulus reaction delay setting in the event that the stimulus reaction delay setting is less than the current amount of time remaining in the countdown to device lock. The reaction delay setting will typically be a much smaller value than the default starting value for the timeout timer – for example it could be between a few seconds to 5 minutes, by way of non-limiting example, compared to 30 minutes to an hour for the default value.

[0035] Thus, the process 200 effectively provides for at least two time-out settings for the time-out timer, a default setting and a shorter stimulus reaction delay setting. The time-out setting is initially set to the default setting, and starts

counting down until either a user interaction with the device 10 occurs, in which case the countdown timer is reset, or until the timer runs out of time, in which case the device locks. In this sense, the device lock process 200 is similar to a traditional lock process. However, unlike in a traditional lock out process, according to embodiments of the current invention if during the lock device timer countdown, an audio or physical stimulus is provided to the user, the timer is reset to the shorter reaction delay setting (assuming that the reaction delay setting is less than the current remaining time on the timer). The user must then interact with the device within the time provided by the shorter reaction delay setting, otherwise the device 10 will lock. It will be appreciated that the steps shown in Figure 2 need not necessarily all be performed in the exact order shown to achieve the desired result.

[0036] Such a device lock configuration can provide an improved level of security for data on the device for some users, as the user stimulus that accompanies such events as newly arrived data is effectively used to monitor the proximity of the user to the mobile device such that the device can be quickly locked if a determination is made that the user is not near the device. The presence of such a feature may give the user the comfort level to extend the length of time for the default time-out setting, thereby decreasing the number of unnecessary lockouts and increasing convenience to the user.

[0037] In an example embodiment, the stimulus reaction delay setting used in process 200 is installed on the device as a preset value that is user configurable. In some example embodiments, the stimulus reaction delay setting can be automatically and adaptively set by the device 10 based on user response characteristics. For example, some users may take only a few seconds to react to a stimulus, whereas other users may habitually take longer time periods such as a few minutes on average – in example embodiments, the stimulus reaction delay setting on a device 10 is periodically adjusted based on the response time of the use of the device. Figure 2 includes in phantom blocks 216, 218 and 220 some steps that are added to process 200 in an example embodiment to effect automatic adaptive adjustment of the stimulus reaction delay setting. As indicated

in step 216, the response times are stored and tracked whenever a user successfully responds to a stimulus, and as indicated in step 218, a lack of user response to a stimulus that leads to a device lock is also tracked. The process 200 includes a sub-process 220 that uses the values tracked and stored in steps 216 and 218 to adjust the stimulus reaction delay setting based on the tracked response times and non-response times of the user of the device. In various embodiments, the stimulus reaction delay setting may, among other things, be adjusted each time the process 200 is started, may be adjusted at set time intervals, may be adjusted when a threshold amount of response time data has been collected since a previous adjustment, and/or may be adjusted when the tracked values fall outside of predetermined boundaries relative to the current stimulus reaction delay setting. In some embodiments, the user may be prompted to determine if they want to accept an adjusted value as the new stimulus reaction delay setting, or the setting may alternatively be changed without requiring approval from the user.

[0038] Although as noted above the stimulus issued to the user in step 210 will generally includes a non-visual component such as an audio sound and/or a physical stimulus, in some embodiments the only stimulus issued may be a visual stimulus on display 22, for example. In some embodiments, different stimulus reaction delay settings could selectively be used based on the event triggering the stimulus and/or the type of stimulus provided to the user. For example, one type of stimulus (for example a certain audio signal or vibration pattern) may be used for an incoming phone call, whereas a different stimulus is used for a new email message, with the stimulus reaction delay setting applied in step 214 being shorter for a phone call than for a new email, given that people are more inclined to react quicker to a phone call than an new email message.

[0039] Although the process 200 has been described in the context of a mobile device it could alternatively be applied to a desktop computer system as well.

[0040] The lock process 200 is based on certain assumptions about how a user will react to a stimulus when the user is near the device, and the device lock

process 200 attempts to adjust the device lock function based on an assumed location or proximity of the device 10 relative to its user. In some example embodiments, the device lock module 65 is configured to adjust the device lock function based on other location relevant information concerning the device 10.

[0041] In some embodiments, security settings other than or in addition to the device lock countdown timer could be changed depending on a user's reaction to a stimulus. For example, the lock device module 65 could be configured to require different passwords depending on the user's reaction (or lack thereof) - when locking the device in step 212, a determination could be made if the device is being locked subsequent to a user failure to respond to a stimulus, and if so a more complex password be required to unlock the device than would be required if the device lock was occurring for other reasons.

[0042] Reference is now made to device lock process 300 of Figure 3. The device lock process 300 is configured to provide different security settings for device locking based on a perceived location of the device 10. For example, if the device 10 is perceived to be in a safe setting, security settings that are less stringent but more convenient to the user are applied. If the device 10 is perceived to be in an insecure setting, security settings that are more stringent but less convenient to the user are applied.

[0043] As indicated in step 302, a device location is determined. In one example embodiment, among the software applications 58 resident on the device is a locating module 64 for determining a location of the device. The locating module 64 could be part of the device lock module 65, or could be part of another application, or could be a standalone application, among other things.

Depending upon the capabilities of the device 10 and the wireless network within which it operates a location for the device 10 could be determined using a variety of methods of varying accuracy. For example, in one embodiment the locating module 64 tracks the current base station 76 within the wireless network 50 that the device 10 is currently communicating with, and in step 304 the device lock module 65 makes a determination as to whether the device is presently in a secure location or not based on the identity of such base station. In such an

embodiment, the device 10 maintains a list of one or more identifiers which identify one or more base stations 76 that are considered to be associated with a safe area for the device 10. For example, the base station near a person's home may be identified as one of the safe base stations. In other embodiments, more accurate locating algorithms are applied by the locating module 64. For example, in a device equipped with a GPS receiver 70, a fairly specific location of the device 10 can be calculated based on received GPS signals. In some embodiments, location may be determined based on communications that occur through the short range communications system 40 of the device 10. For example, in an work or home environment having a wireless LAN or other short range communications system, the device 10 location can be narrowed down to a relatively small area. In some embodiments, a location of the device 10 relative to a user may be deduced based on whether the user responds to a stimulus within a predetermined duration (similar to process 200).

[0044] If in step 304 a determination is made that the device 10 is not in a secure location, then, as indicated in step 306, one or more security settings used by the device lock module 65 are set to high security values. For example, the device lock module 65 may be configured to accept different predetermined passwords based on the security settings. In step 310, the security settings are set to require a more complex password to unlock the device 10 than would be required in a safe setting. Additionally or alternatively as indicated in step 312, the countdown timer value used to determine the period of user inactivity after which a device lock will occur is set to a shorter duration that would be used in a safe setting.

[0045] As indicated in step 308, in the event that a determination is made in step 304 that the device 10 is in a safe location, security settings for the device can be set to a lower value. For example, as indicated in step 314, a shorter or less complex password could be required to unlock the device, and/or as indicated in step 316, a larger time value could be set for the device lock timer.

[0046] Although process 300 as shown in Figure 3 has only two security classification levels branching out from decision block 304, there could actually

be three or more classification levels each associated with a different physical location of the device and each having different set of associated security settings - for example, "home" settings for when the device is within a predetermined proximity of the user's home, "work" settings for when the device is within a predetermined proximity of the user's work and "other location" settings for when the device is in other locations.

[0047] In some embodiments, the settings used by the device lock module 65 could depend on the location of the device 10 relative to a desktop computer 72. For example, as indicated in Figure 1, in some embodiments the device 10 can communicate through a local interface 74 with a local desktop 72. The interface 74 may for example be a docking station or cradle that physically connects to a serial port 30 or other port of the device 10, or could be a short-range wireless interface for communicating with the short range communications system 40 of the mobile device 10. The device lock module 65 in example embodiments adapts its behaviour depending on whether the device 10 is docked or otherwise in local communication with a desktop computer 72. In this regard, an example process 400 performed by device lock module 65 according to embodiments of the invention is shown in Figure 4. In the embodiment represented by the process 400, the desktop computer 72 is configured to communicate its current lock state (unlocked or locked) to a locally connected mobile device 10, and the mobile device 10 is configured to mirror the lock state of the desktop computer 72.

[0048] Process 400 includes a step 402 of monitoring to determine if the device 10 is locally connected through interface 74 to desktop computer 72. If the device 10 is locally connected to the desktop computer 72, then the lock state of the device 10 is set to be the same as that of the desktop computer (step 404). As indicated in step 406, the device lock module 65 monitors for a change in the lock state of the desktop computer 72 from unlocked (U/L) to locked (L). If the desktop lock state has not changed from unlocked to locked, the device lock module continues to check to see if the device 10 is still locally connected to the desktop computer 72 and if so maintain the device 10 in the same lock state as

desktop computer 72. If, however, in step 406 a change in the lock state of the desktop computer 72 from unlocked to locked is detected, then a preset time delay occurs (step 408) after which a determination is made if the mobile device 10 is still locally connected to the desktop computer 72 (step 402), and if so, then the mobile device 10 will also lock up (step 404). The delay in step 408, which may by way of non-limiting example be in the range of a few seconds to a few minutes, is provided to allow a user time to lock their desktop computer and then remove their mobile device 10 from its docking station (thereby severing the local connection with desktop computer 72). If the user does not remove their mobile device 10 from its docking station within the delay provided in step 408, an assumption is made that the user is leaving or has left the device 10 unattended with the desktop computer 72 and so it is then immediately locked. In a further example embodiment, as part of delay step 408, a question to the user is displayed in a user interface window on the mobile device 10 asking if the user wants to lock the device. If the user does not reply within the delay time confirming that the device should not be locked, then the process continues to step 402 and will lock the mobile device if it is still connected to the desktop. If, however, the user confirms within the delay time that they do not want the mobile device locked, then the mobile device will ignore the locked state of the desktop and rely on its own internal device lock timer instead.

[0049] It will be appreciated that processes 200, 300 and 400 can in various embodiments be performed independently of each other, or in some embodiments can be combined and either performed in parallel with each other or sequentially with each other. For example, in process 300 the security settings set based on device location could include the timer default value used in step 202 of process 200 and/or the stimulus reaction delay value used in step 214. Although the above description has focussed on adoption of settings for a device lock process, settings for other applications on the device 10 could also be adaptively configured based on perceived or actual changes in the real or relative position of the mobile device 10. For example, in various example embodiments, the mobile device 10 includes among software applications 58 an instant

messaging module 67 and/or an email filtering module 66. In an example embodiment, the general status setting used by the instant messaging module 67 is set automatically based on a determined location of the device 10 – for example status settings of “user is home”; “user is at work”; or “ user is away, etc. could be automatically selected based on device location. Similarly, email filter settings associated with filtering module 66 are automatically adapted to apply different filtering criteria based on device location – for example, the filter settings in a user home location may be designed to filter out notifications for work-related emails. In the case of adaptive instant messaging and email filtering, the changes in settings or user location need not be communicated to an external server, thus ensuring the user privacy is not a concern.

[0050] The above-described embodiments of the present invention are intended to be examples only. Alterations, modifications and variations may be effected to the particular embodiments by those skilled in the art without departing from the scope of the invention, which is defined by the claims appended hereto.